



Lime Tree Primary Academy

Online Safety Policy

Created on: 22nd July 2015

Updated on 14th July 2023

Online Safety Leads: Natasha Benton, Debbie Rea

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents, FoLT (PTA).

Safeguarding is a serious matter; at Lime Tree Primary Academy we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety or eSafety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Lime Tree Academy School website and school blog; upon review all members of staff will sign as read and understood both the Online Safety Policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Headteacher Name: Clare Larkin

Chair of Governors: Daniel Jagger

Next review Date: July 2024 – or in response to updated guidance/incident

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of online safety at the school who will.
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.
 - Chair the Online Safety Committee

Our appointed governor is **Rhian Baguley**

Head of School

Reporting to the governing body, the Head of School has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Lead.

The Head of School will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Lead has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.

Online Safety Lead

The day-to-day duty of Online Safety Lead is devolved to *Debbie Rea (DSL)* and *Natasha Benton (Computing Lead)*

The Online Safety Leads will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head of School.
- Advise the Head of School, governing body on all e-safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail (CPOMS).

- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Head of School and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Jamie Bates, ESI Tech

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any e-safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head of School.
 - Regularly test Internet Filtering (once monthly)
 - Passwords are applied correctly to all users regardless of age.
 - The IT System Administrator password is to be changed in the case of a breach.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head of School.
- Any online safety incident is reported to the Online Safety Lead (and an Online Safety Incident Report is made via CPOMS), or in their absence, to the Head of School. If you are unsure, the matter is to be raised with the e-Safety Officer or the Head of School to make a decision.
- The reporting flowcharts contained within this online safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters and regular updates with parents regarding any incidents, parents will be taught strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will be sent the student Acceptable Use Policy at the start of each academic year.

Online Safety Committee

Chaired by the Governor responsible for online safety, the Online Safety Committee is responsible:

- to advise on changes to the online safety policy.
- to establish the effectiveness (or not) of online safety training and awareness in the school.
- to recommend further initiatives for online safety training and awareness at the school.

Technology

Protecting children online from inappropriate content

The DfE Meeting digital and technology standards in schools and colleges March 2023 states that:-

“Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It’s important that the right people are working together and using their professional expertise to make informed decisions.”

Lime Tree Primary Academy uses a range of devices including PC’s, laptops, Apple Macs and iPads. In order to safeguard the students and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – We use Securly, a firewall appliance, this is cloud based and is managed by ESI Tech and overseen by the school. This prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Lead, Online Safety Lead and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head of School.

Blocking and Unblocking Online Content – The decision to block and unblock certain websites will be presented to the Online Safety Lead alongside Lime Tree’s SLT and a decision will be made as to whether the website or app is appropriate. This will then be communicated with our ICT Technical Support Staff who will unblock the site.

BYOD (Bring your own device) – Only Lime Tree owned devices can be connected to the school Wifi network. Staff members and members of the school community will not be given access to the Wifi password. Any persons wishing to access internet for school use will borrow a school device (this includes student teachers and supply teachers). Where it is deemed necessary for Wifi to be added to an external device, a decision will be made by the Head of School to assess the risk to this decision.

Internet Monitoring – Securly flags up any inappropriate website access to our Head of School and Online Safety Lead via email notification. In order to access the internet on a laptop, all children and staff have a unique login. The exception to this is in EYFS and KS1 where children use a generic log in for their year group and are observed using equipment by an adult. This allows for the Head of School to see what has been searched online and by whom.

The Head of School and Online Safety Lead will look at the content and what was searched prior to it. Appropriate action will be taken to determine the context of this search. The schools Child Protection Policy will be followed if need be at this point.

We also conduct a monthly test on or around the 15th of each month where we assess Securly's effectiveness by testing with inappropriate key word searches (supervised by a member of staff). Staff are aware of the importance of reporting any inappropriate content that may have become accessible immediately. This is then logged and acted upon via CPOMs, using the 'library' section of CPOMs.

Email Filtering – we use Office 365 alongside Google Apps which removes known spam / virus emails from the users mailbox. It prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that leave site do not hold personal data, staff store this data in the cloud using the school's Office 365 and Google Apps, the documents on here have passwords that only relevant staff are made aware of. No data is to leave the school on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head of School immediately. The Head of School will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's. All staff iPads are password protected.

Passwords – All staff and students (dependent on Key Stage) will be unable to access any computer and iPad without a unique username and password. Staff and student passwords will change if there has been a compromise. Jamie Baites is responsible for the changing of passwords where necessary. When using Safari, children will need to log in using their own personal log in. An exception to this is EYFS, Year 1 and Year 2 who will have adult supervision whilst using the internet. They will log in with a first name but with no password. Staff using their 'Teacher Macbook' are responsible for changing their own passwords and their internet usage is monitored when onsite. Staff use at home is outlined in the Staff AUP.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head of School if there are any concerns. All USB peripherals such as keydrives are not used in school, If ever there is a need to use it must be scanned for virus's first.

Curriculum Content – Our Computing Curriculum outlines Lime Tree's approach to educating children on the four areas of risk online - content, contact, conduct and commerce. These are broken down in to age appropriate expectations for each year group. Online safety lessons will take place each half term. In addition to this, lessons and discussions will be planned in responses to any incidents that occur.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online Safety Policy and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Radicalisation - Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people. Staff and students are prohibited from accessing any websites or social network pages that promote such views. The school has systems and filtering in place to block extremist material and monitor those who attempt to access it. Any persons deemed to be accessing extremist material will be reported to the relevant authorities. Children are taught within the curriculum about propaganda.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – There are many social networking services available; Lime Tree Primary Academy is fully supportive of social networking as a tool to update parents and carers on their children's learning and to celebrate and showcase Lime Tree Primary Academy with a wider audience. The following social media services are permitted for use within Lime Tree and have been appropriately risk assessed

- Twitter – used by the school as a broadcast service (see below).
- Instagram – Use by Class Teacher's to share updates on children's learning.

In addition, the following is to be strictly adhered to:

- Permissions (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and/or surname.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed as soon as possible.

Incidents - Any online safety incident is to be brought to the immediate attention of the Internet Safety Lead, or in their absence, the Head of School. The Internet Safety Lead will assist you in

taking the appropriate action to deal with the incident and an online report must be logged, no matter how small the incident may appear, using CPOMS.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Lime Tree Primary Academy will have an annual Internet Safety training, which is suitable to the audience. This is part of the school's September INSET training day.

Internet Safety training for Children- Internet safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Lime Tree Primary Academy have adapted a set of objectives, based on the National Curriculum for Computing. These objectives have also taken in to consideration the DfE's KCSIE as well up-to-date issues and new technologies or Apps as they arise. This outlines what must be taught each year by the Class Teacher.

Every half term, children will have at least one session regarding internet safety in addition to responsive sessions, which will be planned for following an incident or arising from children's online interests.

As well as the Inset day training, we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Lead is responsible for recommending a programme of training and awareness for the school year to the Head of School and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head of School for further CPD.

Being online and Child Protection

Online sexual violence and sexual harassment between children

Our Head of School and DSL have accessed and understood the DfE [Keeping children safe in education](#) 2022 guidance, specifically part five, 'Child-on-child sexual violence and sexual harassment.'

Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.

Lime Tree Primary Academy recognises that sexual violence and sexual harassment between children can take place online. Examples may include;

- Non-consensual sharing of sexual images and videos
- Sexualised online bullying
- Online coercion and threats
- 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
- Unwanted sexual comments and messages on social media

- Online sexual exploitation

If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- immediately notify the DSL and act in accordance with our child protection and anti-bullying policies.
- if content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.

"If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in [Keeping children safe in education](#)."

- provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy.
- inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make referrals to partner agencies, such as First Response and the Police.
- if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Lime Tree Primary Academy recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

Lime Tree Primary Academy recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, Lime Tree Primary Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

Youth produced sexual imagery (“sexting”)

Lime Tree Primary Academy recognises youth produced sexual imagery (also known as “sexting”) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) and the local [UKCCIS](#) guidance: “Responding to youth produced sexual imagery”.

- Youth produced sexual imagery or ‘sexting’ is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
- It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

Lime Tree Primary Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
 - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
- send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- act in accordance with our child protection policies and the relevant local procedures.
- ensure the DSL (or deputy) responds in line with the [UKCIS](#) and [UKCCIS](#) guidance.
- Store any devices containing potential youth produced sexual imagery securely
 - If content is contained on learners personal devices, they will be managed in accordance with the DfE [‘searching screening and confiscation’](#) advice.

- If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the [UKCIS](#) guidance.
 - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
- review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Lime Tree Primary Academy recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- Lime Tree Primary Academy will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will ensure that the '[Click CEOP](#)' report button used to report online child sexual abuse is visible and available to parents and other members of our community. This can be accessed on our school website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
 - act in accordance with our child protection policies.
 - store any devices containing evidence securely.
 - If content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
 - if appropriate, make a referral to First Response Trafford social care and inform the police via 101, or 999 if a learner is at immediate risk.
 - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
 - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
 - provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

- review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Lime Tree Primary Academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
 - act in accordance with our child protection policy and the relevant KSCMP procedures.
 - store any devices involved securely.
 - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - ensure that the DSL (or deputy) is informed.
 - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk.
 - ensure that any copies that exist of the image, for example in emails, are deleted.
 - report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
 - ensure that the DSL (or deputy) is informed.
 - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk.

- inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
 - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
 - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on Lime Tree provided devices, we will:
 - ensure that the Head of School and DSL is informed in line with our managing allegations against staff policy.
 - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
 - quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Lime Tree Primary Academy. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy. See our bullying policy on our school website.

Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Lime Tree Primary Academy and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Head of School will be informed immediately, and action will be taken in line with the child protection and allegations policies.
- All staff will be up-to-date with 'Prevent training.

Acceptable Use Policy – Staff



Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the online safety officer and CPOMS report completed. Internet access on school devices is limited to accessing information linked to your role in school.

Social networking – is allowed in school in accordance with the internet safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff, student or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device. Your laptop must have a unique password that you have set.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head of School who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of mobile phones – Mobile phone usage is permitted in school but is limited to the staff room or rooms away from children (or classrooms when children are not present). No images should be taken or stored on a personal mobile phone. Personal mobile phones may be used on school trips for phone calls and text messages. Extenuating circumstances where access is needed must first be approved by the Head of School.

Use of WIFI – No personal devices should be connected to the school WIFI.

Monitoring of Internet Usage – All internet usage is monitored by the Head of School and Online Safety Lead. Any material accessed on school devices may also be monitored.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head of School. Permission must be sought stating the reason for using personal equipment.

Viruses and other malware - any virus outbreaks are to be reported to the Online Safety Lead as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Online Safety – like health and safety, online safety is the responsibility of everyone to everyone. As such, you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with students.

Incident reporting - I understand that I must report any concerns about online safety to the Online Safety Leads, the DSL or the Head of School, logging incidents using CPOMS.

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of “stranger danger” when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else’s work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

Y5/6 Only - I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission. If I am allowed, I still have to follow all the other school rules if I use them.

- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.

I understand that if I do not follow these rules, there will be consequences. This might include loss of access to the school network/internet, parents/carers being contacted and, in the event of illegal activities, involvement of the police.

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet
- I will be kind to others when online and when using the equipment



Lime Tree Primary Academy

BRIGHT FUTURES EDUCATIONAL TRUST

Lime Tree Primary School

Budworth Road, Sale,
Cheshire M33 2RP

0161 905 0790

admin@ltpa.bright-futures.co.uk

www.limetree.bright-futures.co.uk

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your child. At Lime Tree we use the internet to gather information, collaborate and communicate.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorises websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school. As a result, we may occasionally monitor these logs. We will inform you if any inappropriate or concerning material has been accessed. this occurs.

At the beginning of each school year, we explain the importance of Internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please arrange to speak with Mrs Benton (our Online Safety Lead).

Your child will be taught about online safety throughout the year and will be asked to agree to the Acceptable Use Agreement (see attached document). Throughout the year, we will respond to any incidents or new technologies/social media that may arise.

Yours Sincerely

Mrs Benton

Risk Log

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	2	2	Online Safety Lead IT Support
2.	Internet browsing	Access to inappropriate/illegal content - students	1	2	2	
5.	Twitter/Instagram	Unknown or inappropriate followers	2	2	4	Class Teachers
6.	Twitter/Instagram	Images of children under child protection or without permission	1	3	3	Class Teachers
7.	Twitter/Instagram	Slandorous or negative comments posted online	2	3	6	Class Teachers Head of School

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 - 3 = **Low Risk**

4 - 6 = **Medium Risk**

7 - 9 = **High Risk**

Owner: The person who will action the risk assessment and recommend the mitigation to Head of School and Governing Body.
Final decision rests with Head of School and Governing Bod

Risk Assessment

Risk No.	Risk
1	Internet Browsing - Access to inappropriate/illegal content - staff
Likelihood	Staff take their laptops home for planning and making resources. They may link up to their own ISP (internet service provider). They may have different filters. This means some inappropriate or illegal sites could be accessed.
1	
Impact	The impact to the school reputation would be high. Staff could access illegal or inappropriate sites and this could lead to the school network being compromised (through virus').
2	
Risk Assessment	Low Risk
Risk Owner/s	Online Safety Lead IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the user will receive the same level of Internet filtering at home as he/she gets whilst in school.</p> <p>Education: Staff are informed of acceptable usage of their laptop at home and will sign an agreement.</p>

Approved / Not Approved (circle as appropriate)

Date:

Signed (Headteacher) :

Signed (Governor) :

Risk No.	Risk
1	Internet Browsing - Access to inappropriate/illegal content - students
Likelihood	We have a filtering system preventing inappropriate searches. Sometimes sites and images can still pass through this system. This could mean that children see inappropriate images or websites.
1	
Impact	The impact to the school reputation would be medium risk. Parents and children may be distressed by what has been seen.
2	
Risk Assessment	Low Risk
Risk Owner/s	Online Safety Lead IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: We have a filtering system that is age appropriate for the users of the computers. In the event that a website has been accessed, this will be reported immediately to our technical support staff who will block the site.</p> <p>Education: Parents are made aware of systems school has in place. Parents would be contacted should an incident arrive.</p>

	Children have to log in to use the internet on laptops and so searches can be traced.
	A monthly test is conducted to check the effectiveness and strength of our filtering system.

Risk No.	Risk
5	Inappropriate followers on Instagram/Twitter
Likelihood	All staff have access to their own Instagram account for their year group. As a result, people could follow classes, staff and parents may then have access to Instagram pages that are inappropriate.
2	
Impact	Staff and parents could be contacted by inappropriate Twitter/Instagram pages.
2	
Risk Assessment	Medium Risk
Risk Owner/s	Online Safety Lead IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Staff are to check followers and block if they appear inappropriate. Education: Children are not to post or access twitter/Instagram under any circumstances. This is a form of communication that is led by the class teacher.

Risk No.	Risk
6	Images of children without permission or under child protection posted online (Twitter/Instagram)
Likelihood	Class Teachers and staff are aware of children who are not allowed to have their images online. Images of these children could end up online accidentally.
1	
Impact	Safety of children under child protection could be compromised.
3	
Risk Assessment	Medium Risk
Risk Owner/s	Online Safety Lead IT Support
Mitigation	Technical: Staff are informed during training regarding posting children's images online. Staff are not to use children's names with children's images.

Risk No.	Risk
7	Slandorous comments on social media.
Likelihood	Every class and the school have an Instagram account and school has a Twitter account. Comments and notifications can appear.
2	
Impact	School reputation could be affected.
3	
Risk Assessment	Medium Risk
Risk Owner/s	Online Safety Lead

	IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Staff are to monitor comments and delete any inappropriate comments. Staff are to only comment on pages of other school classes or pages used for educational purposes.</p> <p>Education: Children cannot access instagram posts within school.</p>

